Architecting and Development of the SecureCyber: A SCADA Security platform Over Energy Smart Grid

Shahir Majed
Advance Informatics School,
Universiti Teknologi Malaysia,
Shahir.majed@mimos.my

Suhaimi Ibrahim
Advance Informatics School,
Universiti Teknologi Malaysia,
suhaimiibrahim@utm.my

Mohamed Shaaban
Centre of Electrical Energy
Systems
Universiti Teknologi Malaysia,
m.shaaban@fke.utm.my

ABSTRACT

This paper documents the design and implementation of the platform while proposing cyber attack scenarios which will have high impact towards grid operations. In addition, we document the results of an initial cyber vulnerability assessment to evaluate the security posture assessment of the current design.

Categories Subject Descriptors

[C.2.0] **Computer-Communication Networks:**
Security and Protection

[C.2.1] **Network Architecture and Design:** Distributed Networks

[D.4.6] **Security and Protection:** Access Control

[K.6.5] **Security and Protection:** Physical Security

General Terms

Design, experimentation, performance

Keywords

Vulnerability Assessment, Smart Grid Security, Security Metrics, Critical Infrastructure Protection.

1. INTRODUCTION

The Supervisory Control and Data Acquisition (SCADA) systems used to control the power grid differ substantially from their typical information technology counterparts. Wide geographic distribution, stringent availability requirements and a heavy reliance on legacy systems introduces significant cyber security concerns while constricting the feasibility of many security controls. Recent NERC Critical Infrastructure Protection (CIP) standards heavily emphasize cyber

security concerns and specifically address requirements to identify critical assets and perform vulnerability assessments against those assets[10]. These concerns have produced an increasing requirement for SCADA specific cyber security education and research. The government has addressed the need for a large-scale test environment through the MIMOS National SCADA Test Bed (NSTB)[8], however students and researchers have limited access to such facilities. The SecureCyber platform provides a multi-functional platform that can be used to provide educational opportunities for students entering power and security fields. The SecureCyber also provides an environment where researchers can explore solutions to security concerns. The SecureCyber platform implements industry standard SCADA software and field devices to provide an authentic control system representation. The SCADA components utilize prevalent control system protocols such as DNP3 and IEC 61850 to perform monitoring and control of the field devices. From a power flow perspective the lab implements a variable load through an overcurrent protection relay which provides an accurate source of control system data. The integration of an actual power flow through the platform ensures attacks can be evaluated for real world impact. The SecureCyber was implemented as a graduation requirement project or University Teknologi Malaysia and Alstom engineering seniors. This effort was a collaboration between both electrical and computer engineering students and faculty. The students developed an understanding of SCADA hardware and software from professional SCADA integrators and used that knowledge to configure the SecureCyber. Next they explored and documented potential cyber vulnerabilities within the lab environment. The NERC CIP requirements were used as a basis for vulnerability assessment strategy. This paper will detail the efforts and resulting lessons learned from the procurement, modeling, and configuration of a functional SCADA platform.

2. PREVIOUS WORK

Multiple universities are either proposing or implementing SCADA platform, however most rely primarily on simulation capabilities which are cheaper and easier to maintain. Giani documented research on simulation-based platform development utilizing

© 2014 Association for Computing Machinery. ACM acknowledges that this contribution was authored or co-authored by an employee, contractor or affiliate of a national government. As such, the Government retains a nonexclusive, royalty-free right to publish or reproduce this article, or to allow others to do so, for Government purposes only.

iiWAS '14, December 04 - 06 2014, Hanoi, Viet Nam Copyright
2014 ACM 978-1-4503-30015/14/12...\$15.00
<http://dx.doi.org/10.1145/2684200.2684308>

Mathworks Simulink and Stateflow toolkits to model the control activities of RTUs and other SCADA components [1]. Davis evaluates a testbed based on a PowerWorld power system simulation tool and the Real-time Immersive Network Simulation Environment (RINSE) tool for network simulation [2]. Jung introduces architecture for security platform and provides steps for performing a basic vulnerability assessment of the environment [11]. Bergman presents a high level architecture for platform development which integrates simulation, emulation and implementation techniques [4]. In addition, Bergman addresses potential connectivity between local and remote SCADA implementation based platform. The SecureCyber platform differs from these platform as it implements industry standard power grid software and hardware to control an actual power flow.

3. SECURECYBER ARCHITECTURE

A key problem faced when implementing a SCADA platform is producing an accurate representation of the interdependencies between the power and cyber components. The simulation of a realistic power system is imperative to accurately evaluate the effectiveness of cyber attacks and defenses. The implementation of the cyber infrastructure must reflect realistic configurations to ensure that platform vulnerabilities closely resemble vulnerabilities in actual SCADA systems. The architecture utilized in the SecureCyber lab mirrors well established SCADA models such as the Basic SCADA Communication Topologies documented in the NIST Industrial Control System Security publication[9] and also other proposed platform architectures[1] [11]. Figure 1 displays the current SecureCyber architecture. The following sections will provide additional documentation of both the power and cyber components.

Figure 1: SecureCyber Platform Architecture

3.1 SCADA Smart Grid Architecture

The current SCADA platform environment replicates two substations controlled by a control center. The control center utilizes a pair of Human-Machine Interface (HMI) systems to control and monitor the substations. The HMIs are implemented as hot swappable spares to accurately model real world redundancy capabilities. Substations are modeled with an overload protection relay connected to software-based remote terminal units (RTUs).

Software	Hardware
Primary HMI server	VPN Devices (2)
Secondary HMI server	Overcurrent Protection Relays (2)
Historian	Autotransformers (2)
Software-based RTU (2)	
Relay programmer (2)	

Table 1: Standard SCADA Equipment

The relays can be monitored and controlled by either the HMIs in the control center or by the local substation computer. Finally, a historian system is used to aggregate audit data produced by the control server. Table 1 lists the individual components included in the SecureCyber platform. The grid power flow model attempts to reflect the basic reliability operations in a substation. The power circuit is intended to imitate transmission lines in an actual power system and includes a power source, an autotransformer and a load. An overcurrent relay is a protective device that is connected to transmission lines through a current transformer. The relays monitor the current flowing through the circuit and protect the transmission lines during short circuit fault conditions and other surges. As the SecureCyber deals strictly with low currents, the relays can be directly connected to the circuit. The relay continually monitors the current through a line to ensure it maintains an acceptable threshold. Once the current exceeds the threshold, the relay trips causing the associated circuit breaker to open.

The current flowing through the test circuit is varied using an autotransformer. The current flowing through the circuit, which is measured using the relays, provides an analog point that can be monitored in the HMI. The HMI will produce an alarm anytime this point surpasses its set threshold. This alerts the operator about the occurrence so mitigating actions can be taken.

3.2 Design Architecture

The design of the cyber architecture provides an equally important role in the SecureCyber platform model. Producing a realistic cyber architecture requires an accurate representation of the protocols used in real world systems as well as the impact that cyber attacks

may have on power flow. The SCADA servers and RTUs operate on traditional x86 architecture desktop systems. SCADA software is installed on either Microsoft Windows 7Pro operating systems. These installations are kept current on service packs and patch levels. While this may be not be representative of a real world scenario, it ensures attacks emphasize SCADA specific system functions instead of traditional IT attack vectors. The SecureCyber platform implements TCP/IP model for network communications. While real world SCADA implementation would likely include both TCP/IP and OSI network models, the restriction to one model simplifies implementation. Ethernet is currently used for the data link/physical network layers. Although it is common for SCADA systems to implement a broad array of physical layer technologies such as RS-232 and various wireless protocols, the pervasiveness of Ethernet simplifies connectivity constraints and improves lab re-configurability. While the SecureCyber operates on a single Ethernet LAN, a realistic SCADA implementation may have a significant geographical distribution. The control center would likely be maintained in an employee facility while the substations are dispersed across the distribution region. In order to represent the long range SCADA communication, specialized VPN devices are used to protect communications between the control center and substations. The use of these tailored VPN devices provides a real-world approach to long range communication protection since legacy SCADA devices typically do not natively support encryption. These devices can also perform basic packet filtering functions to restrict potentially malicious traffic from accessing the substations network segments. The HMIs, RTUs, control servers and relays all communicate across common SCADA protocols. Both IEC 61850 and the Distributed Network Protocol (DNP3) are heavily used protocols in substation automation and are the primary technologies used to perform control communication in SecureCyber. The controls servers and RTUs communicate with the DNP3 while the RTUs and relays communicate with the IEC 61850 protocol.

3.3 Cyber/Power Impact Scenarios

A successful cyber attack against a power system will likely target power flow operations. In order to determine critical assets and provide a basis for establishing attack goals we have proposed impact scenarios. These scenarios address high level attack objectives which will either directly or indirectly affect power production. Likely impact scenarios for this lab environment include the following.

- Reconfiguring a relay
- DDos to systems/devices
- Modifying/disrupting valid alarms
- Producing fake alarms

- Sending incorrect commands to relay
- Manipulating readings from a relay
- Injecting incorrect data to historian

Attempts to execute one of the scenarios will first require that an attacker gain access to some set of system resources. This will require an understanding of known exploitable vulnerabilities within the environment. Vulnerabilities will be determined through a comprehensive vulnerability assessment. The results of this assessment along with the impact scenarios can be combined to produce a set of attack trees. The establishment of attack trees can then be used to determine the attack practicality and evaluate the effectiveness of various defensive mechanisms[3].

Systems	Open Ports (Device 1/Device 2)	Vulnerabilities (Device 1/Device 2)
Relays	2/2 TCP	1/1 High Low 10/10
RTUs	11/11 TCP	3/3 Medium Low 20/21
HMIs	10/24 TCP	2/2 Medium Low 33/33
VPN Devices	1/1 TCP	12/15 Low
SCADA Server	2/1 TCP 2/1 UDP	13/15 Low

Table 2: Port/Vulnerability Scanning Results

3.4 Initial Cyber Security Evaluation Results

In order to evaluate the initial SCADA platform security posture assessment, a rudimentary tool-based vulnerability assessment was performed. This effort was carried out to obtain a stronger understanding of network services and protocols used in the environment and determine system components which might be particularly vulnerable to attack. The tools used in this assessment were limited to Wireshark for network traffic analysis[7], Nmap for port scanning[5] and Nessus for vulnerability scanning[6].

The first step in the security evaluation was an analysis of open ports. Open ports provide both an understanding of current system communication protocols as well as potential attack vectors. Nmap scans were first performed against all TCP ports on each system to determine potential services, UDP ports were ignored during this step due to additional time requirements. After all TCP ports were scanned, the next step involved utilizing Wireshark to determine which ports appear to be used for control specific communication. Wireshark provides the ability to sniff and analyze all network traffic. Using Wireshark we were able to evaluate the DNP3 and IEC 61850 data streams used to transmit devices control information. Finally, vulnerability scanning was performed using the Tenable

Nessus Security Scanner. While vulnerability scanning software can only detect sets of publicly available vulnerabilities, it is useful in determining if well known and easily exploited vulnerabilities may exist on the systems.

During the assessment only one high level vulnerability was found due to a default password. Most other vulnerabilities fell into a category of security best practice violations like information disclosure and unnecessary open ports. The quantitative results of the security analysis are provided in Table 2.

The result of this initial security analysis provides some interesting analysis based on NERC CIP requirements. NERC CIP 007-1 requirement R8.2 states that “only ports and services required for operation” should be enabled on systems. However, scan results showed systems with up to 20 open TCP ports. Since it is unlikely that all open these ports are required for proper operation, this provides one potential compliance violation. Additionally, the default password provides another potential violation against requirement R5.2.1 which requires the “removal, disabling, or renaming” of default accounts.[10] The SecureCyber security posture evaluation is a continuing effort. The next step in the process will address more in-depth review of network protocols and services. This will involve analysis of encryption protocols, authentication, access control mechanisms, and application input validation capabilities. The results of this continual assessment will be compared with NERC CIP requirements as well as other security best practices.

4. FUTURE WORK

4.1 Configuration Management

Configuration management is an often overlooked component in security platform development. SecureCyber development is inexpensive from both a financial and time perspective. Research environments also maintain high knowledge turnover due to continually graduating students. In addition, a failure in a SCADA specific hardware or software components cannot be easily analyzed due to the heavy use of proprietary technology and may require additional funding to obtain vendor guidance. While configuration management should be a concern in any SCADA environment, the emphasis on cyber security evaluation increases this concern as both successful and unsuccessful cyber attacks can leave systems in a degraded state. The analysis of cyber attacks and implementation of potential defense strategies will significantly stress the platform desired configuration. While configuration management for traditional IT systems has been thoroughly studied, maintaining a consistent configuration of SCADA platform will provide a challenge. The SecureCyber platform is currently reviewing solutions to address configuration management requirements.

4.2 Simulation Expansion

The two substation model limits the ability to evaluate the effects of large scale cyber attacks. While the current architecture integrates actual SCADA field devices, future efforts can leverage the integration of both implementation-based and simulation-based platform models similar to the architecture proposed by Bergman[4]. Although attacks against purely simulation-based systems lack authenticity, the integration of actual SCADA devices can be used to provide control variables for the simulation-based results.

5. CONCLUSIONS

The student and faculty efforts have successfully implemented a realistic SCADA security platform. The implementation of industry standard SCADA field devices and software ensures the results of security assessments and attack evaluations will accurately reflect the risk in the modern electric grid. The implementation of a power flow model provides a representational example of how cyber attacks against SCADA systems could affect real world energy distribution. The implementation process provided students with a novel learning environment and also introduces capabilities for expanded research opportunities. Current SecureCyber platform research activity focuses on exploring the security posture of the individual SCADA components and analysis against current NERC CIP cyber security requirements. While initial vulnerability assessment efforts have raised some interesting security concerns, future efforts will provide a more comprehensive analysis of security controls.

6. ACKNOWLEDGEMENTS

This research is funded by the Research University grant of Universiti Teknologi Malaysia (UTM) under the Vot no. 03H74. The authors would like to thank the Research Management Centre of UTM and the Malaysian ministry of education for their support and cooperation including students and other individuals who are either directly or indirectly involved in this project.

7. REFERENCES

- [1] Annarita Giani, Gabor Karsai, Tanya Roosta, et al. A Testbed for Secure and Robust SCADA Systems. ACM SIGBED Review, 5(2), July 2008.
- [2] C. M. Davis, J. E. Tate, H. Okhravi, et al. SCADA Cyber Security Testbed Development. Proc. 38th North American Power Symposium, pages 483–488, September 2006.
- [3] Chee-Wooi Ten, Manimaran Govindarasu, Chen-Ching Liu. Vulnerability Assessment of Cybersecurity for SCADA Systems using Attack Trees. IEEE Power Engineering Society General Meeting, 2007.
- [4] David C. Bergman, Dong Jin, David M. Nicol, Tim Yardley. The Virtual Power System Testbed and Inter-Testbed Integration. 2nd Workshop on Cyber Security Experimentation and Test, August 2009.

- [5] <http://nmap.org>. Nmap Security Scanner.
- [6] <http://www.nessus.org/nessus/>. Nessus.
- [7] <http://www.wireshark.org>. Wireshark: A Network Protocol Analyzer.
- [8] MIMOS MicroEnergy Lab: National SCADA Test Bed: Fact Sheet, 2007.
- [9] Keith Stouffer, Joe Falco, Karen Scarfone. NIST SP800-82: Guide to Industrial Control Systems (ICS) Security. Technical report, National Institute of Standards and Technology, September 2008.
- [10] North American Electricity Reliability Council. NERC Critical Infrastructure Protection (CIP) Reliability Standards, 2009.
- [11] S. K. Sungmo Jung, Jae-gu Song. Design on SCADA Test-bed and Security Device. International Journal of Multimedia and Ubiquitous Engineering, 3(4), October 2008.